

2015 10th International Conference on Malicious and Unwanted Software (MALWARE 2015)

**Fajardo, USA
20 – 22 October 2015**



**IEEE Catalog Number: CFP1559F-POD
ISBN: 978-1-4673-8472-8**

**Copyright © 2015 by the Institute of Electrical and Electronic Engineers, Inc
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

******This publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1559F-POD
ISBN (Print-On-Demand):	978-1-4673-8472-8
ISBN (Online):	978-1-5090-0319-8

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Session 1 – Broad Spectrum Malware, Defense Strategies and Mechanisms

Using Inherent Command and Control Vulnerabilities to Halt DDoS Attacks	3
<i>Lanier Watkins, Kurt Silberberg, Jose Andre Morales and William H. Robinson</i>	
Deep Neural Network based Malware Detection using Two Dimensional Binary Program Features	11
<i>Joshua Saxe and Konstantin Berlin</i>	
Run-Time Classification of Malicious Processes using System Call Analysis	21
<i>Raymond Canzanese, Spiros Mancoridis and Moshe Kam</i>	

Session 2 – Broad Spectrum Malware, Defense Strategies and Mechanisms

Variant: A Malware Similarity Testing Framework	31
<i>Jason Upchurch and Xiaobo Zhou</i>	
A Framework for Empirical Evaluation of Malware Detection Resilience Against Behavior Obfuscation	40
<i>Sebastian Banescu, Tobias Wüchner, Aleieldin Salem, Marius Guggenmos, Martín Ochoa and Alexander Pretschner</i>	
Automatically Combining Static Malware Detection Techniques	48
<i>David De Lille, Bart Coppens, Daan Raman and Bjorn De Sutter</i>	

Session 3 – Mechanisms and Strategies to Thwart Attacks

Segmented Sandboxing – A Novel Approach to Malware Polymorphism Detection	59
<i>Fernando C. Colón Osorio, Hongyuan Qiu and Anthony Arrott</i>	
Sandboxing and Reasoning on Malware Infection Trees	69
<i>Krishnendu Ghosh, Jose Andre Morales, William Casey and Bud Mishra</i>	
Covert Remote Syscall Communication at Kernel Level: A SPOOKY Backdoor	74
<i>Florian Kerber, Dominik Teubert and Ulrike Meyer</i>	
Gorilla Sniffs Code Similarities, The Case Study of Qwerty versus Regin	82
<i>Guillaume Bonfante, Jean-Yves Marion and Fabrice Sabatier</i>	

Session 4 – The Measurement Problem: Inherent Limitations of Current Measurement Frameworks

Measuring the Information Security Risk in an Infrastructure	93
<i>Ferenc Leitold, Kálmán Hadarics, Eszter Oroszi and Krisztina Gyórfy</i>	
Measuring the Health of Antivirus Ecosystems	101
<i>Fanny Lalonde Lévesque, Anil Somayaji, Dennis Batchelder and José M. Fernandez</i>	
Stealthy Malware Traffic – Not as Innocent as It Looks	110
<i>Xingsi Zhong, Yu Fu, Lu Yu, Richard Brooks and G. Kumar Venayagamoorthy</i>	

Session 5 – Mechanisms and Strategies to Detect Mobile Malware

GroddDroid: A Gorilla for Triggering Malicious Behaviors	119
<i>A. Abraham, R. Andriatsimandefitra, A. Brunelat, J.-F. Lalande and V. Viet Triem Tong</i>	
Clustering Android Malware Families by Http Traffic	128
<i>Marco Aresu, Davide Ariu, Mansour Ahmadi, Davide Maiorca and Giorgio Giacinto</i>	
Targeted DoS on Android: How to Disable Android in 10 Seconds or Less	136
<i>Ryan Johnson, Mohamed Elsabagh, Angelos Stavrou and Vincent Sritapan</i>	
Counterfeit Mobile Devices – The Duck Test	144
<i>John O'Brien and Kimmo Lehtonen</i>	